Mimecast Integrations

Introduction

The Mimecast integration collects events from the Mimecast API.

Assumptions

The procedures described in Section 3 assumes that a Log Collector has already been setup.

Requirements

Configuration

Authorization parameters for the Mimecast API (Application Key, Application ID, Access Key, and Secret Key) should be provided by a Mimecast representative for this integration. Under Advanced options you can set the time interval between two API requests as well as the API URL. A Mimecast representative should also be able to give you this information in case you need to change the defaults.

Note: Rate limit quotas may require you to set up different credentials for the different available log types.

Logs

Audit Events

This is the mimecast.audit_events dataset. These logs contain Mimecast audit events with the following details: audit type, event category and detailed information about the event. More information about these logs.

DLP Logs

This is the mimecast.dlp_logs dataset. These logs contain information about messages that triggered a DLP or Content Examination policy. More information about these logs.

SIEM Logs

This is the mimecast.siem_logs dataset. These logs contain information about messages that contains MTA (message transfer agent) log – all inbound, outbound, and internal messages.

Threat Intel Feed Malware: Customer

This is the mimecast.threat_intel_malware_customer dataset. These logs contain information about messages that return identified malware threats at a customer level. Learn more about these logs.

Threat Intel Feed Malware: Grid

This is the mimecast.threat_intel_malware_grid dataset. These logs contain information about messages that return identified malware threats at a regional grid level. More about these logs.

TTP Attachment Logs

This is the mimecast.ttp_ap_logs dataset. These logs contain Mimecast TTP attachment protection logs with the following details: result of attachment analysis (if it is malicious or not etc.), date when file is released, sender and recipient address, filename and type, action triggered for the attachment, the route of the original email containing the attachment and details. Learn more about these logs.

TTP Impersonation Logs

This is the mimecast.ttp_ip_logs dataset. These logs contain information about messages containing information flagged by an Impersonation Protection configuration.

TTP URL Logs

This is the mimecast.ttp_url_logs dataset. These logs contain Mimecast TTP attachment protection logs with the following details: the category of the URL clicked, the email address of the user who clicked the link, the url clicked, the action taken by the user if user awareness was applied, the route of the email that contained the link, the action defined by the administrator for the URL, the date that the URL was clicked, url scan result, the action that was taken for the click, the description of the definition that triggered the URL to be rewritten by Mimecast, the action requested by the user, an array of components of the message where the URL was found. More about these logs.

Mimecast Integration Procedures

Please provide the following information to CyTech:

Mimecast API

1. Application Key - Specifies application key for user.

2. Application ID - Set the Application Id.

3. Access Key - Set Access Key.

4. Secret Key - Set Secret Key.

Revision #2
Created 23 April 2024 13:36:08
Updated 19 June 2024 06:54:01